Newcastle University

Code of Connection (CoCo) for Devices Connected to the University’s Network

Author	Information Security Officer (Technical)
Version	V1.1
Date	23 April 2015

Code of Connection (CoCo) for Devices Connected to the University's Network

Introduction

This Code of Connection (CoCo) establishes a minimum security baseline for devices connected to Newcastle University's ICT network. By following the guidance in this Code of Connection you are helping the University reduce its exposure to risks that may:

- Impact the University's ability to comply with its legal, regulatory and contractual obligations.
- Impact the confidentiality, integrity and availability of sensitive information assets and information systems.

Scope

This Code of Connection supports the **Information Security Policy** and **Data Protection Policy** by establishing a minimum security baseline for the following types of device:

- Server
- Network *(e.g. routers, switches, wireless access points, etc.)*
- End-point *(e.g. personal computers, kiosks, etc.)*
- Peripheral *(e.g. printers, plotters, scanners, multi-function devices, etc.)*
- Backup *(e.g. tape libraries, network attached storage, etc.)*
- Other – non-traditional computing devices *(e.g. scientific and medical equipment, smart devices, Internet of Things (IoT), Building Management Systems (BMS), Industrial Control Systems / Supervisory Control and Data Acquisition (ICS/SCADA, etc.)*

This Code of Connection does not cover BYOD (Bring Your Own Device) or encryption for mobile devices. Separate guidance on BYOD and mobile device encryption is available to download from the following location:

- **Information Security Web Pages**
  http://www.ncl.ac.uk/itservice/security/

Remember - confidential and sensitive information must be encrypted if stored on a portable computing device or portable storage device.

Target Audience

This Code of Connection is for everyone who installs, manages or maintains ICT equipment connected to Newcastle University's ICT network. This includes central and local ICT support, administrative and academic staff, and students who are involved in these activities.

Reserved Powers

We (Newcastle University's IT Service) will disconnect a device from the University's network if we believe it poses a risk to ICT security. We will always try to contact the device owner before disconnecting a device.

Comments and questions

If you have any comments or questions about how to comply with this Code of Connection, then please contact the Information Security Team through the IT Service Desk by telephone **(0191 208) 5999** and by email at **it.servicedesk@ncl.ac.uk**

Code of Connection (CoCo) for Devices Connected to the University's Network

High-Level Information Security Requirements

1.0	**Device Registration**
1.1	You must register all devices you are responsible for in the Network Inventory before connecting them to the University's network.
1.2	You must keep registration details up to date.
1.3	DHCP should be used for address assignment, where possible.
Note:	By correctly registering a device, and by keeping those registration details up to date, you are helping us provide a faster response to ICT security incidents by allowing us to easily identify the device owner. You can register devices through the IT Service Desk by email at **it.servicedesk@ncl.ac.uk**. You can also register devices through your **local ICT support**. If you don't register a network device, or keep the registration details up to date, then we may disconnect that device from the University's network.

2.0	**Public IP Addresses**
2.1	You should give us a valid business reason before connecting a device to the public (128.240.) network.
Note:	By giving us a valid business reason you are helping us to stop the connection of unsecure devices to the public network (e.g. printers). If you don't give us a valid business reason, then we may not allow you to connect the device to the public network.

3.0	**Redundant Devices**
3.1	You should disconnect devices from the campus network when they are no longer needed.
Note:	Redundant devices are often forgotten about and are at risk of losing their security settings and not having the latest security updates installed. By disconnecting redundant devices you are helping us to reduce the number of devices that could be used by a hacker to disrupt and compromise the University's ICT services. We will disconnect redundant devices from the University's network if they pose a risk to ICT security.

4.0	**Vulnerability Scanning**
4.1	We (Newcastle University's IT Service) will scan devices connected to the campus network for vulnerabilities.
4.2	You should fix non-secure devices within 5 working days of receiving a notification from the IT Service.
Note:	By fixing vulnerabilities you are helping us to reduce the risk of hackers using those vulnerabilities to gain control of devices and using those devices to disrupt and compromise the University's ICT services. If you don't fix a vulnerable device that poses a risk to ICT security, then we will disconnect that device from the University's network.

5.0	Malware Prevention
5.1	You should install and maintain anti-malware software on all devices that are vulnerable to malicious software (e.g. viruses, worms, bots, Trojans, adware, spyware, ransomware and scareware).
Note:	Malicious software can cause significant damage and disruption to ICT services. By using good anti-malware software, and by keeping that software up to date, you are helping us to reduce this risk. We will disconnect devices from the University's network if they become infected with malicious software.

6.0	Security Updates
6.1	You should install the latest vendor security updates on all firmware, operating systems and applications.
6.2	If a legacy application dictates the use of a non-secure platform that cannot be upgraded, then you should contact the Information Security Team through the IT Service Desk for further advice: **telephone**: (0191 208) 5999 **email**: it.servicedesk@ncl.ac.uk
Note:	By installing the latest security updates you are fixing vulnerabilities that could be used by a hacker or malicious software to attack the device. Devices that are no longer in receipt of vendor security updates may have vulnerabilities that cannot be fixed. If a legacy application dictates the use of a non-secure platform that cannot be upgraded, then we may be able to recommend alternative ways to secure that platform. If it is not possible to secure the platform, then the platform should be retired or replaced. You should consider replacement costs as part of your on-going operational costs. We will disconnect devices from the University's network if they are vulnerable to attack.

7.0	Management of Network Services
7.1	You should turn off unsecure and unnecessary network services.
7.2	Network services should not be running with administration or root privileges, where possible.
Note:	Unsecure and unnecessary network services could be used by a hacker or malicious software to attack a device. If those services are running with administration privileges then a hacker could use them to compromise other services running on the device. Services such as rlogin, rsh, rpc, telnet and ftp are not designed for secure use and need to be replaced with more secure alternatives such as ssh, scp and sftp. Other services (e.g. nfs, cifs, samba, MySQL, MS-SQL, Apache, IIS, etc.) may be vulnerable to attack if they are not securely configured. We will disconnect devices from the University's network if they are running vulnerable network services. Please refer to **Appendix A** for more information on managing network services.

8.0	Software Firewalls
8.1	Software firewalls should be running and securely configured on all devices connected to the public (128.240.) and internal (10.) network, where possible.
Note:	Software firewalls that are configured to use a default deny policy for all in-bound traffic can help prevent hackers from exploiting vulnerabilities in network services that you may have missed when securing the device. By using a default deny policy, you can limit all in-bound network traffic to trusted network protocols and ports. Commercial software firewalls may also provide basic IDS (Intrusion Detection System) and DLP (Data Leakage Prevention) capabilities. We will disconnect devices from the University's network if they are running vulnerable network services.

9.0	Access Control
9.1	You should password protect administration consoles.
9.2	You should change vendor default passwords.
9.3	You should disable vendor installed guest accounts and other unnecessary accounts.
9.4	Restrict remote root and administrator access to trusted hosts (e.g. PCs belonging to system administrators, etc…), where possible.
9.5	Authenticate remote root and administrator access with two-factor authentication (e.g. if you are using SSH, then consider using a private key with a passphrase), where possible.
9.6	You should only use disk file systems that support Access Control Lists (e.g. NTFS).
9.7	You should not export network file systems (such as NFS and CIFS) with anonymous write permissions.
9.8	You should not allow anonymous uploading to FTP servers.
Note:	**Protecting Console Access** Password protected consoles provide a first-line of defence against attacks. Hackers and automated hacking tools will often use vendor default passwords, guest accounts and other unnecessary accounts to gain access to a device. Restricting root and administrator logons to trusted hosts and using two-factor authentication can help reduce the risk posed by brute-force password attacks. **Access Control Lists** File system ACLs can help prevent further compromise of a device if a low privilege account is compromised by stopping the attacker from accessing sensitive system files and files belonging to other users. **Network File Systems & FTP Servers** Criminals have been known to store illegal materials on devices that are running non-secure network file systems and non-secure FTP servers. We will disconnect devices from the University's network if they do not have secure access controls.

10.0	Hardening
10.1	You should secure all devices, operating systems and applications in accordance with vendor recommendations.
Note:	By securing your devices in accordance with vendor recommendations you are helping to reduce other risks that might not have been explicitly addressed through this Code of Connection (e.g. risks that are unique to a particular hardware or software product). Vendors will normally publish security guidance on their web sites. We will disconnect devices from the University's network if they have not been secured in accordance with vendor recommendations.

11.0	**Obfuscation** (reducing public technical information)
11.1	Change default network service banners and SNMP (Simple Network Management Protocol) community strings, where possible.
Note:	By changing default service banners and SNMP community strings you are helping to reduce the threat posed by hackers. Service banners and SNMP community strings are used to advertise the types of services running on a device and will often include distribution and version information. Hackers will often use this information to identify devices that are vulnerable to attack. We will disconnect devices from the University's network if they are advertising services that are vulnerable to attack.

12.0	Software Sources
12.1	You should only install software from trusted sources.
Note:	Hackers will try to trick you into downloading software that has been tampered with. The compromised software may include keystroke loggers, back doors, spam bots and other types of malicious software. To reduce this risk, all software needs to be obtained from trusted sources. Trusted sources include software vendors, authorised resellers and recognised open source community web sites. We can help you verify the authenticity of a source. If possible, verify downloaded software with an appropriate hash algorithm such as MD5 (Message-Digest Algorithm). We will disconnect devices from the University's network if they are running software that has been modified by a hacker.

13.0	Quality Assurance
13.1	You should check security settings for misconfigurations after system changes and at least annually if no changes have been made.
Note:	Devices that have been previously configured for security may have had their security settings wiped or modified because of software upgrades, system restores or other technical changes. Security settings may have also been corrupted over time. By checking security configurations after a system change and annually you are helping to identify and remove vulnerabilities that could be exploited by a hacker. We will disconnect devices from the University's network if they are vulnerable to attack.

14.0	Web Applications
14.1	You should use HTTPS to protect web sessions that send and receive authentication data and other people's personal information.
14.2	You should sign HTTPS connections with digital certificates obtained from a trusted Certificate Authority such as the Janet Network.
14.3	You should protect web forms and URLs against injection and XSS (Cross Site Scripting) attacks.
14.4	You should encrypt or hash passwords and other people's personal information if it is stored in a database.
14.5	Authentication to web applications should use the shibboleth SSO (Single Sign On) system, where possible.
Note:	**HTTPS and Digital Certificates** HTTPS is used to encrypt sensitive and confidential information when sent across open networks. A digital certificate obtained from a trusted source (such as the Janet Network or other recognised Certificate Authority) can provide confirmation to the customer that the web site is owned and operated by the University. HTTPS and digital certificates can help reduce the risk of sensitive and confidential information being intercepted by eavesdroppers or accidentally sent to web sites that are operated by fraudsters. **Injection Vulnerabilities** Injection vulnerabilities can be used by hackers to access and modify web applications and databases. XSS (Cross Site Scripting) attacks can be used to deface web sites, hijack user sessions, and redirect users to malicious web sites. Information on how to avoid injection and XSS (Cross Site Scripting) attacks can be obtained from organisations such as **OWASP (The Open Web Application Security Project)**. **Database Encryption** By encrypting or hashing sensitive and confidential information that's stored in a database-driven web site, you are helping to reduce the risk of that data being accessed by hackers if they successfully attack your database server. It is important to remember that encrypted data can still be accessed in an unencrypted form if the web application is vulnerable to injection attacks.

15.0	Data Protection
15.1	If your device is used to collect, store and/or process other people's personal information, then you must protect that information in compliance with the Data Protection Act.
15.2	If disposing of ICT equipment, then you must use only methods of data destruction that are proven to be secure and render data recovery impossible.
Note:	**Data Protection Act** The Data Protection Act states that other peoples personal information must: 1. Be processed fairly and lawfully 2. Be collected only for a specific purpose 3. Not be excessive 4. Be accurate 5. Not be kept longer than needed 6. Be processed in line with the rights of the data subject 7. Be protected 8. Be protected to European Economic Area standards if sent overseas The Information Security Team delivers Data Protection Training through the Staff Development Unit. **Secure Data Disposal** It may be possible for criminals to recover data that has been previously deleted. You can reduce this risk by contracting a secure data disposal company to dispose of your redundant ICT equipment and to provide documented evidence of data destruction (e.g. a data destruction certificate). Secure deletion software can also be used on individual devices. If you require further advice on the Data Protection Act or secure data disposal then please contact the Information Security Team through the IT Service Desk: **telephone**: (0191 208) 5999 **email**: it.servicedesk@ncl.ac.uk

16.0	Wireless Access Points
16.1	You should not connect wireless APs (Access Points) to the campus network.
Note:	Unauthorised wireless APs (Access Points) can be used by hackers to access and compromise internal ICT services. If your work area does not have good wireless coverage then please notify the IT Service Desk: **telephone**: (0191 208) 5999 **email**: it.servicedesk@ncl.ac.uk We will disconnect wireless APs from the University's network if they are vulnerable to attack or interfere with the University's wireless service. For any end-user wireless access point connected to the campus network (including student owned wireless access points), all traffic entering the campus network from that device will be considered the responsibility of the owner of that device (registered owner in the network inventory, or the tenant of a student room where the device is located).

17.0	Forensic Readiness
17.1	You should enable system, security and application logs and retain them for at least three months or as required.
Note:	By enabling and retaining system, security and application logs, you are helping us to improve our ability to detect and investigate ICT security incidents.

18.0	Incident Reporting
18.1	You should report all suspected information security incidents to the IT Service Desk. The IT Service Desk will forward your report to the Information Security Team.
Note:	IT Service Desk **: telephone**: (0191 208) 5999 **email**: it.servicedesk@ncl.ac.uk

Code of Connection (CoCo) for Devices Connected to the University's Network

Appendix A
Non-secure network services

A non-secure service is a network service that is:

- Not required for the functioning of a network connected device;
- Or, has been replaced with a more secure alternative

For example:

- A web server should only run services needed for the purpose of the device (e.g. a LAMP stack)
- SSH and SFTP should be used instead of telnet and FTP

We recommend that you run a port scan using Nmap against the devices that you manage and check if any services are not needed or have been replaced with more secure alternatives.

Nmap needs to be run from a remote computer and can be downloaded from your Linux repository or nmap.org if you use a Windows PC.

The following Nmap command will perform a TCP and UDP scan against your remote host and will generate a list of network services that may need to be shut down or hardened:

```
nmap -sS -sU -T4 -O <scan-target>
```

<scan-target> is the IP address or DNS name of your remote host. **Do not run Nmap against any hosts that you do not manage.**

As a rule of thumb, if you don't know what a particular network service does, turn it off and document the change. The network service can be re-enabled if turning it off impacts the device.